WHAT IS CLAIMED IS:

1. A cryptographic system with at least one server and any number of clients, including none, the cryptographic system further comprising:

at least one application on one of the at least one server, each capable of engaging in a context-free multi-part communication session with any of the clients;

a key repository process on one of the at least one server, the key repository process configured to validate and record authorizations of specific programs to access one or more than one set of symmetric keys, wherein each of the at least one application is configured to query the key repository process for one or more than one set of symmetric keys, and the key repository process further configured, in response to the query from a particular instance of the at least one application, to provide the requested one or more than one set of symmetric keys to the particular instance of the at least one application but only if the key repository process authenticates the particular instance of the at least one application as being pre-authorized to receive the requested one or more than one set of symmetric keys;

wherein, the particular instance of the at least one application can utilize the one or more than one set of symmetric keys for securely off-loading sensitive information in any intermediate part of the context-free multi-part communication session.

2. The cryptographic system as in claim 1, wherein the sensitive information in an intermediate part is securely off-loaded to a database.

3. The cryptographic system as in claim 1, wherein the sensitive information in an intermediate part is securely off-loaded as a cookie to an intended one of the clients that returns the cookie within a next part of the context-free multi-part communication session.

4. The cryptographic system as in claim 1, wherein the key repository process maintains one set of symmetric keys for all of the at least one application.

5. The cryptographic system as in claim 1, wherein the key repository process maintains a distinct set of symmetric keys for each one of the at least one application.

6. The cryptographic system as in claim 1, wherein the text-free multi-part communication session is conducted using a hypertext transfer protocol.

7. The cryptographic system as in claim 1, wherein both the at least one application and the at least one server utilize one of a hypertext markup language, a standard generalized markup language, and an extensible markup language.

8. The cryptographic system as in claim 1, wherein the securely off-loaded sensitive information can be then accessed by any one of the at least one application engaging in the context-free multi-part communication session.

9. The cryptographic system as in claim 1, wherein the securely off-loaded sensitive information is encrypted.

10. The cryptographic system as in claim 1, wherein the sensitive data is securely off-loaded to a working memory in a server to enable a single server process instance to service all communications between the at least one application and the server.

11. The cryptographic system as in claim 1, wherein the at least one application includes instances of the same application.

12. The cryptographic system as in claim 1, wherein the key Repository process is a process pair.

13. A method for secure context-free multi-part communication in a computer system with a server and any number of clients, including none, the method comprising:

instantiating at least one application on the server, each capable of engaging in a context-free multi-part communication session with any of the clients;

instantiating a key repository process on the server, so that

the key repository process validates and records authorizations of specific applications to access one or more than one set of symmetric keys, wherein each of the at least one application is configured to query the key repository process for one or more than one set of symmetric keys, and

in response to the query from a particular instance of the at least one application, the key repository process provides the requested one or more than one set of symmetric keys to the particular instance of the at least one application but only if the key repository process authenticates the particular instance of the at least one application as being pre-authorized to obtain the requested one or more than one set of symmetric keys;

wherein, the particular instance of the at least one application utilizes the one or more than one set of symmetric keys for securely off-loading sensitive information in any intermediate part of the context-free multi-part communication session.